(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 658 021 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
28.03.2001 Bulletin 2001/13

(51) Int Cl.[7]: **H04L 9/08**, H04L 9/32

(21) Application number: **93480219.0**

(22) Date of filing: **08.12.1993**

(54) **A method and system for key distribution and authentication in a data communication network**

Verfahren und System zur Schlüsselverteilung und Authentifizierung in einem Datenübertragungssystem

Procédé et système de distribution de clé et authentification dans un réseau de communication de données

(84) Designated Contracting States:
DE FR GB

(43) Date of publication of application:
14.06.1995 Bulletin 1995/24

(73) Proprietor: **International Business Machines Corporation**
Armonk, N.Y. 10504 (US)

(72) Inventors:
- **Bjorklund, Ronald Einar**
  F-06510 Gattières (FR)
- **Bauchot, Frédéric**
  F-06640 Saint Jeannet (FR)
- **Wetterwald, Michèle Marie**
  F-06800 Cagnes Sur Mer (FR)
- **Kutten, Shay**
  Rockaway, NJ 07866 (US)
- **Herzberg, Amir**
  Bronx, NY 10471 (US)

(74) Representative: **de Pena, Alain**
Compagnie IBM France
Département de Propriété Intellectuelle
06610 La Gaude (FR)

(56) References cited:
US-A- 5 199 072

- **COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, vol.9, no.2, April 1990, AMSTERDAM NL pages 145 - 152 DOMINGO-FERRER 'Security Network Bootstrapping: An Algorithm for Authentic Key Exchange and Digital Signatures.'**

EP 0 658 021 B1

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the Invention

[0001] This invention deals with key distribution and authentication in a data communication network, and more particularly with key authentication in a wireless LAN type of network.

Background of the Invention

[0002] Conventional data communication networks include a host station or network manager providing network control by being connected to a network including one or several node stations, which, in turn concentrate and manage the traffic provided from/to remote terminal stations. In principle, several terminal stations are attached to each node station, such as to provide a sub-network which can be referred to as a cell.

[0003] One such network to be more particularly considered in this invention may be defined as a wireless Local Area Network (LAN). Such a network to be disclosed in details in the following description includes remote stations connected to individual nodes or base stations, via radio links with the base station(s), in turn, connected to a host (or network) manager (herein also referred to as wireless manager) via a wired LAN circuitry.

[0004] But regardless of be the network architecture, the data traffic must be protected as the system poses increasing threats to the security of communications and operations involving end-users and network components.

[0005] This problem has already received particular attention from the data communication industry sector. In fact, security is a must, and customers always include this feature in defining their requirements or network functional characteristics. One may easily understand their concern on the matter when bearing in mind that in such networks the flow of data carries very sensitive proprietary information relating to the customers company operation, e. g., cash-flows, prices, correspondence within the network, requests from their own customers, etc...

[0006] One essential function for achieving security in such a network is a mechanism to reliably authenticate the exchange of messages between communicating parties. This involves the establishment of a session key, which key needs being distributed safely.

[0007] One such system has been described by S.P. Miller, B.C. Newman, J.I. Schiller and J.H. Saltzer, as the "Kerberos Authentication and Authorization System" of the M.I.T. Project Athena, Cambridge, Massachussets, December 1987. The proposed system requires using physical protection and synchronization operations. This is however troublesome and a heavy burden to carry when it addresses private networks made for non-technical customers wishing to minimize their own implications on the network buildup. Besides, it adds to the original cost of the network and therefore makes the proposed network installation less competitive. Other approaches involve using so-called public key cryptography operations which are computationally expensive and imply the need to compute and store in a Key Distribution Center, all the Public key / Private key couples prior to the stations initializations.

[0008] In some cases public keys are provided to all station attaching to the network, by using carrying security personnel which is both heavy to handle and expensive.

[0009] Another approach requires each station to be initialized in a secure central location before being shipped to their destination. This is again an expensive process, especially if the customer has to do it.

[0010] US-A-5 199 072 discloses a method for registering a user module with a LAN. The module selects a key and a polynomial for encrypting data in response to a password received from the LAN.

Summary of the Invention

[0011] One object of this invention is to provide a method and system for key authentications which is both safe in an insecure network environment while being easy to be operated by a non-professional user. Another object of this invention is to provide such a method for a so-called wireless LAN network combining both wireless communications with wired LAN.

[0012] Still another object of this invention is to provide a method for distributing private keys needed in an authentication procedure of a wireless LAN remote and base stations.

[0013] These and other characteristics, objects and advantages of this invention will become more apparent from the following description made with reference to the attached figures.

Brief description of the Figures

[0014] Figure 1 represents a wireless LAN topology with a two-level hierarchical network structure the invention should be applied to.

[0015] Figure 2 represents the complete network including a network manager and showing the various items and

parameters to be used for the invention.

[0016] Figure 3 (including fig.3a and 3b) figure 4 (including fig.4a and 4b) figure 5 and figure 6 are flow charts for implementing the invention.

Description of the Preferred Embodiment of the Invention

[0017] This description shall refer to a so-called wireless LAN.

[0018] It should, however, already be understood, that the wireless LAN to be described herein in further details as to those characteristics requested for the invention, should in no way be considered to be limitative. For instance, one should understand that the invention obviously applies to different kinds of network architectures, be they wireless or wired.

[0019] However, just for the sake of simplifying this description and defining clearly the inventive concept the description shall refer to a best mode of implementation made according to the topology represented in the attached figures.

[0020] Let's first consider a wireless LAN topology with a two-level hierarchical network structure, as represented in figure 1. The whole geographical area to be covered by the communication network is divided into cells. Associated with each cell is a base station 1, 2 etc, that is connected to a backbone network and acts as access point or relay, to a number of remote (mobile) stations 3, 4, 5, 6, 7 individually communicating with one base station over a wireless channel. The number of remote stations may vary throughout time, some leaving and others attaching to the network. Also, the individual cells topography may vary since any individual mobile station may gain access to the network via any of the several base stations.

[0021] Typically, a mobile station registers with one of the base stations to gain access to the network. All communications between the mobile station and other entities are subsequently handled by the base station with which it was registered.

[0022] As an example, one may consider the environment of an industrial campus consisting of several office buildings. The buildings are divided into cells, which cells are connected via some backbone network such as a wired LAN (e. g. Ethernet/token ring). Mobile stations such as portable computer terminals which can operate both indoor and outdoor with limited range, use a wireless link to access the base stations on the backbone network. Each base station controls the set of mobile stations in its cell.

[0023] The two-level cellular architecture with wireless links and backbone LANs, as considered in the preferred embodiment of this invention offers several advantages. For instance, non-overlapping cells that are some distance apart can have independent transmission access channels without any interference. Hence, the capacity of the system can be significantly increased. In addition, the management functions such as signalling and access protocol for the wireless access channel can be simplified greatly since each cell can be operated independently. But this architecture should in no way be construed as limiting the scope of this invention which, as will become apparent from the following description, obviously applies also to any other architecture such as one using a higher number of levels, for instance. The base station itself is actually a router or a bridge between the wireless LAN cell and the LAN backbone and in turn up to a network station or host device. Accordingly, and as represented in figure 2, the complete network shall also include a network station for managing the whole network. Said network manager shall herein be also referred to as Wireless Manager.

[0024] Communications between remote stations (RS) and base station (BS) are performed through Adapter Units each including a cell control device (CC) or more generally software implemented means for performing adapter functions. Each base station is also provided with a wireless control agent (WCA) function, while the network station is provided with a wireless manager (WM) function. Each base and network station is provided with a storage device (DB) including a data base and ROM facilities in the adapters.

[0025] The description of the operation of these devices shall herein be limited to sole implication within the invention.

[0026] The purpose of the invention is to enable performing an authentication process used to verify a station does not usurp the identification of someone else, particularly during network installation. It is performed between a remote station adapter and its corresponding base station adapter, then between the base station and the wireless manager or more generally speaking the network manager (WM).

[0027] During network installation for a given customer, the network manager is first installed. But as per the authentication process, the operations deal with first base installation, then with individual remote stations, and/or the system may proceed with authenticating a second base station (if any), additional remote stations, and so on.

[0028] Represented in figure 3 is a general flowchart of the authentication key distribution method of this invention. The upper line shows the locations and network sub-system concerned with the authentication operations, i. e. : network manager (Wireless Manager), first base station, (mobile) remote station and other base stations (if any). But in addition, the flow chart shows that some operations are performed during the manufacturing of the various network components. For instance, a common key Km (the same for all manufactured adapters) is hidden by being included in the adapter

programmable read-only memory (PROM) at manufacturing level. Also, a unique identifier, so-called Universally Administered Medium Access Control (MAC) address (UA) is also stored in the adapter PROM. This address is unique to an adapter. It may be made function of specific data provided to the manufacturer (e. g. IEEE provided identifier (IEEE address range)).

[0029] Using those adapters, carrying the Km key and UA parameters (see step 10 and 11 in figure 3), one may start performing the operations for authentication key initialization (installation) on the first base adapter. The process includes installing a preliminary key K1 in first base station (step 12), then the first base adapter is triggered to generate a network key Knet and a backbone key Kb (13) using a predefined logical function, from the network key Knet. Said backbone key Kb is sent to the Wireless (network) Manager which stores it into a hidden storage position (steps 14 and 15).

[0030] The process may then proceed with installing mobile remote stations to be attached to the installed base station or installing additional base stations.

[0031] As per the remote stations installation, the system starts with reading the universal address (UA) stored in the remote station adapter PROM (step 16), and, by some predefined way, chooses a name for the considered remote station (step 17). Actually the considered remote station RS user runs a program provided with the adapter, conventionally referred to as the diagnostics program, and this triggers the display of the stored UA data. The remote mobile station name and address indications are forwarded to the network manager WM (step 18), e.g. by telephone, or by any other written/verbal means, to the corresponding operator. The network manager searches into its stored data, for an already installed base (in present implementation that would relate to the first or any already installed and still active network base), and provide it with the received mobile station UA address and name information (step 19) through the installed wired LAN circuits, for instance. The adapter base station encrypts the name by using Knet as an encryption key, to derive Knet(name) which actually stands for E(Knet, name), where E(x) is an encryption function, Knet is used as the encrypting key and name is the encrypted data. This notation will herein be used throughout the following text. The first base adapter also generates a new name parameter, so-called name', by using a predefined logic function using the parameters Knet(name), UA and Km (step 20), then sends name' to the mobile remote station adapter (step 21) via the wireless manager, using a secure protocol. In other words, name' acts as a password provided to the remote station which avoids communicating Knet(name) in clear. The mobile remote station knowing the logic function applied in the corresponding base station, extracts Knet(name) from name' (step 22) and stores it (step 23) safely in some protected memory.

[0032] A similar approach is also used to deal with installing, additional bases (so-called "another" base station), except that in this case, no name data is required.

[0033] When the adapter hardware is installed, the new base station operator retrieves its UA address (step 24) using a conventional diagnostics program. Before configuring the base station, the operator provides this address (UA) to the network administrator at the network manager location (step 25). The network or so-called wireless manager searches for an already installed base (e. g. first base station) and provides it with the said UA parameter (step 26). The installed base station computes an external view of the network key, i. e. Knet', dedicated to the new base station, as a function of Knet, UA and Km (step 27) and sends it to the network manager using a predefined secure (authenticated) protocol. The Knet' parameter is provided to the target base adapter being installed.

[0034] In some cases, the network might be simplified with the Wireless Manager function being installed in the first base station. Accordingly, this might further avoid transporting security data on the LAN backbone. The network key is then entered in the first base station thru a conventionally installed configuration menu.

[0035] In any case the new base station extracts Knet from the received Knet' (step 29) and installs it safely in its base adapter memory (step 30).

[0036] Accordingly the authentication process is also made as safe as possible by avoiding need for forwarding sensitive data in clear, as much as possible.

[0037] More detailed information on first base installation procedure are provided in figure 4.

[0038] The operations start in fact with the network manager receiving a request for first base installation (step 35). A random generator of any known kind is then triggered to compute the preliminary key K1 (step 36) and send it to the base through the LAN wired circuit (step 37).

The reception of K1 is used to trigger the generation of the network key Knet (step 39). This may for example be performed by a conventional random generator simply generating Knet as a random number. The same Knet key shall be used for the whole network. The base station also computes the backbone key (Kb) to be used to encrypt security messages when they flow on the LAN backbone. Kb is derived from Knet. The Wireless Manager (network manager) is then triggered for starting a Kb retrieval process for further use for next base or remote station installation (step 40). To that end, the Wireless Manager sends a first message (AUTH1) to the base station. Upon receiving said message, the base station generates a random number N1 (step 41) and sends it to the Wireless Manager (step 42) through a returning message (AUTH2). The Wireless Manager stores N1 and randomly generates a number N2 (steps 43 and 44). The network manager starts then generating an authentication requesting message on basis similar to those

described by Ray Bird et al in IEEE Journal on Selected Areas in Communications, June 1993, Vol 11 No5 pp 679-693. This message contains as parameter the result of K1(BKEY ⊕ K1(WM' ⊕ K1(N2 ⊕ K1(N1)))).

[0039] More particularly, the network manager starts encrypting N1 with the key K1, performs a logic Exclusive OR (XOR) function, represented by the ⊕ symbol, with N2, encrypts the result with K1 then again performs a XOR function with a parameter WM' (a common parameter also known by the base adapter as the Wireless Manager identifier), re-encrypts with K1, XORes again with a constant data BKEY (defined at manufacturing level and known by each adapter) indicating that the Wireless Manager wants to retrieve the backbone key Kb, and finally encrypts again with K1. The authentication request message AUTH3 shall also include N2 (steps 45, 46).

[0040] This message is forwarded to the first base which extracts and stores N2. Then said first base station performs (step 48) the same operations that were performed in step 45 in order to authenticate the Wireless Manager as the originator of the message. The base station starts computing K1(N2 ⊕ K1(N1)) or in other words encrypts N1 with K1, performs a XOR function with N2, and encrypts the result again with K1 (step 49). Then the backbone key is encrypted with K1 (step 50). And finally K1(K1(Kb ⊕ N2)) is computed in step 51.

[0041] Those authentication parameters are forwarded to the Wireless Manager in an authentication message AUTH4 (step 52).

[0042] The Wireless Manager proceeds to base adapter authentication by computing K1(N2 ⊕ K1(N1)) and comparing the data obtained to the received data (step 53). Then it decrypts the encrypted backbone key to derive Kb therefrom (step 54). It encrypts K1(N2 ⊕ K1(Kb)) using the key K1 (step 55) to enable authenticating the message received from the base station (see step 51). Finally, the Manager deletes K1, N1 and N2 and stores the backbone key in a hidden Manager's memory location (steps 56 and 57).

[0043] Therefore, using a safe authentication protocol, the Wireless Manager has been provided with the backbone key which shall later be useful to installing additional base and remote stations that may be required to build up the complete data network.

[0044] Let's, for instance, proceed with another (i.e. 2 , 3).

base station to be attached to the network. This involves, as already mentioned in connection with figure 3, using the first, or any other installed base station which should already store the network key, Knet, extract Knet, and provide said network key to the base to be installed. For security purposes, Knet is not provided as such but rather encoded into a Knet' parameter derived from using a predefined logic function operated over Knet, the base adapter UA and the key Km installed in each adapter in the PROM containing the code, at manufacturing time. In addition, as already explained with regard to figure 4, authentication parameters are also used to reinforce the transmission security using again a protocol similar to the protocol recommended by Ray Bird et al (see above).

[0045] The "other" new base installation method is described in full details hereunder with reference to figure 5.

[0046] As already mentioned, the new base station operator retrieves its address (UA) using a diagnostics program. It then provides the Wireless Manager with the UA value (step 60). The Wireless Manager chooses an installed base station and contacts it (step 61) with a message AUTH1. This information is used in the base station to trigger a random generator providing a random number N1 (step 62), which is sent to the Wireless Manager in a message AUTH2 (step 63) and stored therein. The reception of N1 triggers the generation of a random number N2 (step 64). The network Manager then initiates the generation of the authentication data to be used for network security checking, i. e.

$$Kb(NKEY \oplus Kb(WM' \oplus Kb(N2 \oplus Kb\ (N1)))). \quad (1)$$

with NKEY set during manufacturing in each adapter to be used in the network (written in the microcode). As a matter of fact, NKEY is defined the same way BKEY was.

[0047] The message AUTH3 including the result of operation (1) and UA and N2 generated in the Wireless Manager, is forwarded to the already installed base selected for delivering Knet information (steps 67, 68).

[0048] The receiving base adapter first authenticates the received message origin (Wireless Manager) by computing :

$$Kb\ (NKEY \oplus Kb\ (WM \oplus Kb\ (N2 \oplus Kb(N1)))) \quad (2)$$

Should the generated data (2) be identical to (1), authentication test is positive (step 69). Otherwise, the process is stopped and a warning is sent to a network administrator.

[0049] The base adapter then computes the following :

$$\text{step 70 : } Knet' = f(Knet, UA, Km) \quad (3)$$

wherein f(x) stands for a predefined logic function performed over the variable x,

$$\text{step 71 : } Kb(N2 \oplus Kb(N1)), \tag{4}$$

$$\text{step 72 : } Kb\,(Knet'), \tag{5}$$

$$\text{step 73 : } Kb(Kb(Knet') \oplus N2). \tag{6}$$

[0050] And the last three parameters are included in an AUTH4 message sent to the Wireless Manager. Said Wireless Manager starts with checking for authenticating the sending base adapter identity, by computing Kb(N2 ⊕ Kb(N1)) in step 75 and comparing the result to the received data (4). Should this test succeed, then the Wireless Manager proceeds with decrypting Kb(Knet') to obtain Knet' (step 76), and use it (step 77) for further authentication by computing Kb(Kb (Knet') ⊕ N2) to be checked for match with (6).

[0051] Then N1 and N2 are deleted (step 78) and Knet' is displayed to the Wireless Manager operator (step 79) to be forwarded (e. g. by telephone), or by any other verbal/written means, to the installator of the new base station. Knet' is entered into said new base adapter which, knowing the inverse function of f(x), derives Knet therefrom, stores it, derives Kb from Knet using the same logic as in the first base station adapter, and deletes Knet'. The new base station is then fully installed.

[0052] Represented in figure 6 is the detailed flow-chart relative to a remote station installation. As mentioned in connection with figure 3, the installations of both remote station or "another" base station (i.e. other than first base station) look very similar to each other, except for the presence of the so-called "name" parameter to be used for remote station installation and not for the "another" base installation.

[0053] Therefore the Wireless Manager (network manager) is provided with the said remote station address UA and name. Since Knet is to be used in the process, the Wireless Manager chooses again any active already installed base station and starts with triggering therein the generation of a random number N1. Said N1 is provided to the Wireless Manager for storage and triggering of random number N2 generation. The network manager initiates again the generation of the authentication data, which now involves using the "name" parameter. The computed data is then :

$$\text{step 80 : } Kb(name \oplus Kb(WM' \oplus Kb(N2 \oplus Kb(N1)))) \tag{7}$$

[0054] The parameters forwarded to the base station now include : UA, N2 and "name" and the result of equation (7) (step 81).

[0055] The receiving base station authenticates the Wireless Manager provenance by performing, as was done for said "another" base station (see above), the logic operations of equation (7) with the received parameters and starts encrypting the name by using the base stored Knet data as an encryption key and computing a name' as a predefined function of (Knet (name), UA and Km) (see step 82).

[0056] Then start the computations of :

Kb(N2 ⊕ Kb (N1))
Kb(name')
Kb(Kb(name') ⊕ N2).

[0057] All these data are included in an AUTH4 message sent to the Wireless Manager. Said Wireless Manager starts with checking for authenticating the sending base adapter identity through computation and authentication of Kb(N2 ⊕ Kb(N1)). It then decrypts Kb(name') and extracts name'. The authentication process proceeds with computation and authentication of the last parameter, Kb (Kb(name') ⊕ N2).

[0058] Once these authentications are declared positive, name' is displayed on the operator's console and forwarded for further use by the remote station which extracts Knet (name) therefrom and stores it.

Claims

1. A method for key distribution and authentication for enabling secure data traffic in a data transmission network wherein remote stations are to be attached to a network manager via at least one base station, said method

including for network installation :

installing a common hidden key Km and a unique individual identifier UA in each station to be used in the network ;

installing a first base station, said installation including :

generating, in said network manager, a preliminary key K1 and installing said K1 key in said first base station ;

using said preliminary key installation to trigger the selection, within said first base station, of a network key Knet and of a derived backbone key Kb, therefrom ;

forwarding said Kb to the network manager and

storing said Kb therein ;

optionally installing "another" base station, said another base installation including :

reading the said another base station identifier UA;

forwarding said another base station identifier UA to said network manager ;

said network manager searching an installed base station and providing said installed base station with said another base station identifier UA ;

computing within said installed base station a parameter Knet' as a predefined logic function of Knet, Km and said another base station identifier UA ;

providing said another base station with said Knet' ;

said another optional base station extracting said network key Knet from said Knet' based on the knowledge of said predefined logic function and storing said network key within said another base station ;

deriving Kb from Knet in the new base station;

installing a remote station, said remote station installation including :

reading said remote station identifier UA ;

choosing a "name" for said remote station ;

providing both said remote station identifier UA

and said name to said network manager ;

said network manager searching an installed base station and providing said installed base station with said remote station identifier UA and said chosen name ;

encrypting within said installed base station, said name with said network key Knet, and computing a name' parameter as a predefined logic function of encrypted name, Km and said remote station identifier UA ;

providing said name' to said remote station, said remote station deriving the encrypted name therefrom, based on the knowledge of said predefined function, and storing said encrypted name into said remote station.

2. A method for key distribution and authentication according to claim 1, wherein said preliminary key K1 is randomly

generated within said network manager.

3. A method for key distribution and authentication according to claims 1 or 2 wherein said network key Knet is randomly generated within said first installed base station.

4. A method for key distribution and authentication according to claim 3, wherein said forwarding the backbone key Kb to the network manager includes encrypting said backbone key Kb with the preliminary key K1 and including said encrypted backbone key into a base authenticating message using predefined parameters known to both the base station and the network manager.

5. A method for key distribution and authentication according to claim 1 wherein said providing said another base station with said Knet' includes encrypting said Knet' with said backbone key Kb and including said encrypted Knet' into a said installed base authentication message using predefined parameters known to both said installed base station and said network manager and providing said authentication message to said network manager.

6. A method for key distribution and authentication according to anyone of claims 1 through 5, wherein said data transmission network is a so-called wireless LAN and said remote stations are individually connected to a given base station via a radio link.

7. A method for key distribution and authentication according to claim 6 wherein said radio link uses the so-called frequency hopping technique with all the remote stations attached to a given base station using a same frequency hopping pattern.

8. A method according to anyone of claims 1 through 7 wherein said first base station is installed within said network manager .

9. A system for key distribution and authentication for enabling secure data traffic in a so-called wireless LAN network wherein remote mobile stations are to be connected through wireless links to a so-called network or wireless manager, via so-called base stations connected to said network manager via a backbone network including a wired LAN, said system being characterized in that it includes :

read-only storage means within each mobile station and base station adapter unit, with a common hidden key Km and an individual identifier UA stored therein during manufacturing;

means for installing a first base station, said means for installing a first base station including :

a random generator for generating within said network manager adapter, a random preliminary key K1 ;

means for forwarding K1 to said first base station adapter ;

means, within said first base adapter, triggered by said K1 key for generating a random network key Knet, and for deriving a Kb parameter therefrom ;

means, within said base station for encrypting Kb with the K1 key, for embedding said encrypted Kb within base authentication parameters known to both the base station and the network manager, and for transmitting said encrypted Kb and authentication parameters to said network manager ; and,

means, within said network manager for extracting and storing Kb after authenticating the originating base station,

and subsequently installing any remote station or any additional or so-called "another" base station by using means for addressing the already installed base station for computing therein a predefined function of, inter alia, network key Knet, and for forwarding the so computed data to the network manager and said any remote station or said "another" base station.

Patentansprüche

1. Ein Verfahren zur Schlüsselverteilung mit Echtheitsnachweis zwecks Ermöglichen eines sicheren Datenverkehrs in einem Datenübertragungsnetzwerk, in dem Fernstationen über mindestens eine Basisstation an einen Netzwerk-Manager angeschlossen werden sollen, wobei das Verfahren der Netzwerkinstallation umfasst:

   Installieren eines gemeinsamen verborgenen Schlüssels Km und eines unverwechselbaren individuellen Identifikators UA in jeder im Netzwerk zu benutzenden Station;

   Installieren einer ersten Basisstation, wobei die Installation umfasst:

      In dem Netzwerk-Manager Generieren eines vorläufigen Schlüssels K1 und Installieren des Schlüssels K1 in der ersten Basisstation;

      Benutzen der vorläufigen Schlüsselinstallation zum Auslösen der Auswahl eines Netzwerkschlüssels Knet und eines daraus abgeleiteten Fernnetzschlüssels Kb in der ersten Basisstation

      Senden des Kb an den Netzwerk-Manager, und

      Abspeichern des Kb darin;

   Wahlweise Installieren einer "anderen" Basisstation, wobei diese andere Basisstation beinhaltet:

      Lesen dieses Identifikators UA der anderen Basisstation;

      Senden des Identifikators UA dieser anderen Basisstation an den Netzwerk-Manager

      wobei der Netzwerk-Manager eine installierte Basisstation sucht und den Identifikator UA dieser anderen Basisstation an diese installierte Basisstation sendet;

      Berechnen, innerhalb dieser installierten Basisstation, eines Parameters Knet' als vordefinierte Logikfunktion von Knet, Km, und des Identifikators UA dieser anderen Basisstation;

      Beliefern dieser anderen Basisstation mit Knet'; wobei diese andere wahlfreie Basisstation den Netzwerkschlüssel Knet aus dem Knet' aufgrund der Kenntnis der vordefinierten Logikfunktion herauszieht und den Netzwerkschlüssel innerhalb dieser anderen Basisstation speichert;

      Kb ableiten von Knet in der neuen Basisstation;

   Installieren einer Fernstation, wobei die Installierung der Fernstation beinhaltet:

      Lesen des Fernstation-Identifikators UA

      Auswählen eines "Namens" für die Fernstation:

      Senden sowohl des Fernstations-Identifikators UA als auch des Namens an den Netzwerk-Manager

      wobei der Netzwerk-Manager eine installierte Basisstation sucht und den Fernstations-Identifikator UA und den gewählten Namen an die installierte Basisstation sendet;

      Verschlüsseln des Namens mit dem Netzwerkschlüssel Knet in der installierten Basisstation, und Berechnen eines Parameters name' als vordefinierte Logikfunktion des verschlüsselten Namens, Km, und des Fernstations-Identifikators UA

      Senden dieses name' an die Fernstation, wobei die Fernstation den verschlüsselten Namen daraus herauszieht aufgrund der Kenntnis der vordefinierten Funktion, und Speichern des verschlüsselten Namens in der Fernstation.

2. Ein Verfahren zur Schlüsselverteilung mit Echtheitsnachweis gemäß Anspruch 1, in dem der vorläufige Schlüssel K1 im Netzwerk-Manager zufallsgeneriert wird.

3. Ein Verfahren zur Schlüsselverteilung mit Echtheitsnachweis gemäß Anspruch 1 oder 2, in dem der Netzwerkschlüssel Knet in der ersten installierten Basisstation zufallsgeneriert wird.

4. Ein Verfahren zur Schlüsselverteilung mit Echtheitsnachweis gemäß Anspruch 3, in dem das Weitersenden des Fernnetzschlüssels Kb an den Netzwerk-Manager beinhaltet das Verschlüsseln des Fernnetzschlüssels Kb mit dem vorläufigen Schlüssel K1 und Einschließen des verschlüsselten Fernnetzschlüssels in eine Basis-Echtheitsnachweis-Meldung, unter Verwendung der vordefinierten Parameter, die sowohl der Basisstation als auch dem Netzwerk-Manager bekannt sind.

5. Ein Verfahren zur Schlüsselverteilung mit Echtheitsnachweis gemäß Anspruch 1, in dem dieses Senden des Knet' an diese andere Basisstation beinhaltet das Verschlüsseln des Knet' mit dem Fernnetzschlüssel Kb und Einschließen des verschlüsselten Knet' in eine installierte Basis-Echtheitsnachweis-Meldung unter Verwendung der vordefinierten Parameter, die sowohl der installierten Basisstation als auch dem Netzwerk-Manager bekannt sind, und Senden der Echtheitsnachweis-Meldung an den Netzwerk-Manager beinhaltet.

6. Ein Verfahren zur Schlüsselverteilung mit Echtheitsnachweis gemäß einem beliebigen der Ansprüche 1 bis 5, in dem das Datenübertragungsnetzwerk ein sogenanntes Drahtlos-LAN ist und die Fernstationen individuell über eine Funkverbindung an eine gegebene Basisstation angeschlossen sind.

7. Ein Verfahren zur Schlüsselverteilung mit Echtheitsnachweis gemäß Anspruch 6, in dem die Funkverbindung die sogenannte Frequenzsprungtechnik benutzt, wobei alle Fernstationen an eine gegebene Basisstation angehängt sind, die das gleiche Frequenzsprungmuster benutzt.

8. Ein Verfahren gemäß einem beliebigen der Ansprüche 1 bis 7, in dem die erste Basisstation innerhalb des obigen Netzwerk-Manager installiert ist.

9. Ein System zur Schlüsselverteilung mit Echtheitsnachweis zum Ermöglichen eines sicheren Datenverkehrs in einem sogenannten Drahtlos-LAN-Netzwerk, in dem ortsbewegliche Fernstationen über drahtlose Verbindungen an einen sogenannten Netzwerk- oder Drahtlos-Manager, über sogenannte Basisstationen durch ein Fernnetzwerk einschließlich eines verdrahteten LAN an den Netzwerk-Manager angeschlossen sind, wobei das System dadurch gekennzeichnet ist, dass es beinhaltet:

   Nur-Lese-Speichermittel in jeder ortsbeweglichen Station und Basisstation-Adaptereinheit, mit einem gemeinschaftlichen verborgenen Schlüssel Km und einem individuellen Identifikator UA, die bei der Herstellung darin gespeichert wurden;

   Mittel zum Installieren einer ersten Basisstation, wobei die Mittel zum Installieren einer ersten Basisstation umfassen:

      Einen Zufallsgenerator zum Generieren eines zufälligen vorläufigen Schlüssels K1 in dem Netzwerk-Manager-Adapter;

      Mittel zum Senden von K1 an den ersten Basisstations-Adapter;

      Mittel innerhalb des ersten Basis-Adapters, die vom Schlüssel K1 ausgelöst werden, zum Generieren eines Zufallsnetzwerkschlüssels Knet, und zum Ableiten eines Parameters Kb von diesem;

      Mittel in der Basisstation zum Verschlüsseln von Kb mit dem Schlüssel K1 zum Einbetten des verschlüsselten Kb in die Basis-Echtheitsnachweis-Parameter, die sowohl der Basisstation als auch dem Netzwerk-Manager bekannt sind, und zum Übertragen des verschlüsselten Kb und der Echtheitsnachweis-Parameter an den Netzwerk-Manager; und

      Mittel innerhalb des Netzwerk-Managers zum Herausziehen und Speichern von Kb nach dem Echtheitsnachweis der Ausgangs-Basisstation;

und anschließend Installieren einer beliebigen Fernstation oder einer zusätzlichen oder einer sogenannten "anderen" Basisstation durch Benutzen der Mittel zum Adressieren der bereits installierten Basisstation zum darin Berechnen einer vordefinierten Funktion des, inter alia, Netzwerkschlüssels Knet, und zum Senden der so berechneten Daten an den Netzwerk-Manager und a diese beliebige Fernstation oder "andere" Basisstation.

Revendications

1. Procédé de distribution de clé et authentification pour permettre un trafic de données sûr dans un réseau de transmission de données dans lequel des stations distantes doivent être connectées à un gestionnaire de réseau via au moins une station de base, ledit procédé incluant pour l'installation du réseau les étapes consistant à :

   installer une clé commune cachée Km et un identificateur individuel unique UA dans chaque station devant être utilisée dans le réseau ;
   installer une première station de base, ladite installation incluant :

   la génération, dans ledit gestionnaire de réseau, d'une clé préliminaire K1 et l'installation de ladite clé K1 dans ladite première station de base ;
   l'utilisation de ladite installation de clé préliminaire pour déclencher la sélection, à l'intérieur de ladite première station de base, d'une clé de réseau Knet et d'une clé de réseau fédérateur dérivée Kb de celle-ci ;
   le réacheminement de ladite Kb au gestionnaire de réseau et
   la mémorisation de ladite Kb à l'intérieur de celui-ci ;

   en option, l'installation d'une "autre" station de base, ladite installation d'une autre base incluant :

   la lecture dudit identificateur UA d'une autre station de base ;
   le réacheminement dudit identificateur d'une autre station de base UA audit gestionnaire de réseau ;
   ledit gestionnaire de réseau cherchant une station de base installée et fournissant à ladite station de base installée ledit identificateur UA d'une autre station de base ;
   le calcul à l'intérieur de ladite station de base installée d'un paramètre Knet' en tant qu'une fonction logique prédéfinie de Knet, Km et dudit identificateur UA d'une autre station de base ;
   la fourniture à ladite autre station de base dudit Knet' ;
   ladite autre station de base en option extrayant ladite clé de réseau Knet dudit Knet' sur la base de la connaissance de ladite fonction logique prédéfinie et mémorisant ladite clé de réseau à l'intérieur de ladite autre station de base ;
   recueillant Kb à partir de Knet dans la nouvelle station de base ;

   installant une station distante, ladite installation de station distante incluant :

   la lecture dudit identificateur UA de station distante ;
   le choix d'un "nom" pour ladite station distante ;
   la fourniture audit gestionnaire de réseau à la fois dudit identificateur UA de station distante et dudit nom ;
   ledit gestionnaire de réseau cherchant une station de base installée et fournissant à ladite station de base installée ledit identificateur UA de station distante et ledit nom choisi ;
   chiffrant à l'intérieur de ladite station de base installée ledit nom avec ladite clé de réseau Knet, et calculant un paramètre de nom' en tant qu'une fonction logique prédéfinie d'un nom chiffré, de Km et dudit identificateur UA de station distante ;
   fournissant ledit nom' à ladite station distante, ladite station distante recueillant le nom chiffré de celui-ci, sur la base de la connaissance de ladite fonction prédéterminée, et mémorisant ledit nom chiffré dans ladite station distante.

2. Procédé de distribution de clé et authentification selon la revendication 1, dans lequel ladite clé préliminaire K1 est générée aléatoirement à l'intérieur dudit gestionnaire de réseau.

3. Procédé de distribution de clé et authentification selon les revendications 1 ou 2, dans lequel ladite clé de réseau Knet est générée aléatoirement à l'intérieur de ladite première station de base installée.

4. Procédé de distribution de clé et authentification selon la revendication 3, dans lequel ledit réacheminement de la clé de réseau fédérateur Kb au gestionnaire de réseau inclut le chiffrement de ladite clé de réseau fédérateur Kb avec la clé préliminaire K1 et incluant ladite clé de réseau fédérateur chiffrée dans un message d'authentification de base utilisant des paramètres prédéfinis connus à la fois de la station de base et du gestionnaire de réseau.

5. Procédé de distribution de clé et authentification selon la revendication 1, dans lequel ladite fourniture de ladite Knet' à ladite autre station de base inclut le chiffrement de ladite Knet' avec ladite clé de réseau fédérateur Kb et incluant ladite Knet' chiffrée dans un dit message d'authentification de base installée en utilisant des paramètres prédéfinis connus à la fois de ladite station de base installée et dudit gestionnaire de réseau et en fournissant ledit message d'authentification audit gestionnaire de réseau.

6. Procédé de distribution de clé et authentification selon l'une quelconque des revendications 1 à 5, dans lequel ledit réseau de transmission de données est un réseau dit LAN sans fil et lesdites stations distantes sont connectées individuellement à une station de base donnée via une liaison radio.

7. Procédé de distribution de clé et authentification selon la revendication 6, dans lequel ladite liaison radio utilise la technique dite à bond de fréquence avec toutes les stations distantes connectées à une station de base donnée en utilisant un même modèle de bond de fréquence.

8. Procédé selon l'une quelconque des revendications 1 à 7 dans lequel ladite première station de base est installée à l'intérieur dudit gestionnaire de réseau.

9. Système de distribution de clé et authentification pour assurer un trafic de données sûr dans un réseau dit LAN sans fil dans lequel des stations distantes mobiles doivent être connectées par l'intermédiaire de liaisons sans fil à un gestionnaire dit de réseau ou sans fil, via les stations dites de base connectées audit gestionnaire de réseau via un réseau fédérateur incluant un LAN câblé, ledit système étant caractérisé en ce qu'il inclut :

un moyen de mémorisation à lecture seulement, à l'intérieur de chaque station de base et unité d'adaptateur de station de base, avec une clé commune cachée Km et un identificateur individuel UA mémorisé à l'intérieur pendant la fabrication ;
un moyen pour installer une première station de base, ledit moyen pour installer une première station de base incluant :

un générateur aléatoire pour générer dans ledit adaptateur de gestionnaire de réseau une clé préliminaire aléatoire K1 ;
un moyen pour réacheminer K1 audit adaptateur de première station de base ;:
un moyen, à l'intérieur dudit adaptateur de première base, déclenché par ladite clé K1 pour générer une clé de réseau aléatoire Knet, et pour recueillir un paramètre Kb de celle-ci ;
un moyen, à l'intérieur de ladite station de base pour chiffrer Kb avec la clé K1, pour incorporer ladite Kb chiffrée à l'intérieur des paramètres d'authentification de base connus à la fois de la station de base et du gestionnaire de réseau, et pour transmettre lesdits Kb chiffrée et paramètres d'authentification audit gestionnaire de réseau ; et,
un moyen, à l'intérieur dudit gestionnaire de réseau, pour extraire et mémoriser Kb après authentification de la station de base source,

et installer ultérieurement une station distante quelconque ou une station supplémentaire quelconque ou une station dite "autre" station de base quelconque en utilisant un moyen pour adressage de la station de base déjà installée afin de calculer ici une fonction prédéfinie de clé de réseau Knet, entre autres, et pour réacheminer les données ainsi calculées au gestionnaire de réseau et à ladite quelconque station distante ou à ladite "autre" station de base.

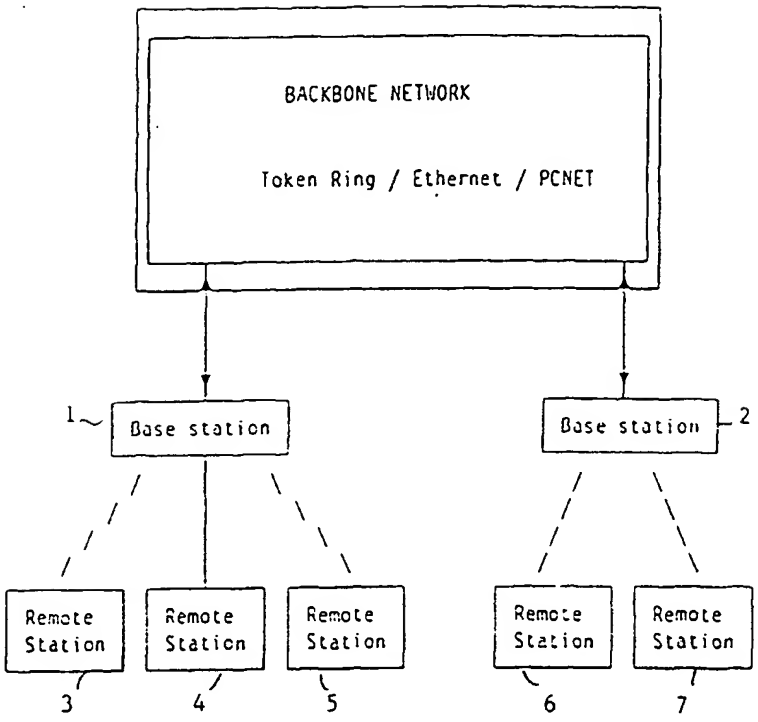
BACKBONE NETWORK
Token Ring / Ethernet / PCNET
1
Base station
Base station
2
Remote Station
Remote Station
Remote Station
Remote Station
Remote Station
3
4
5
6
7

FIGURE 1

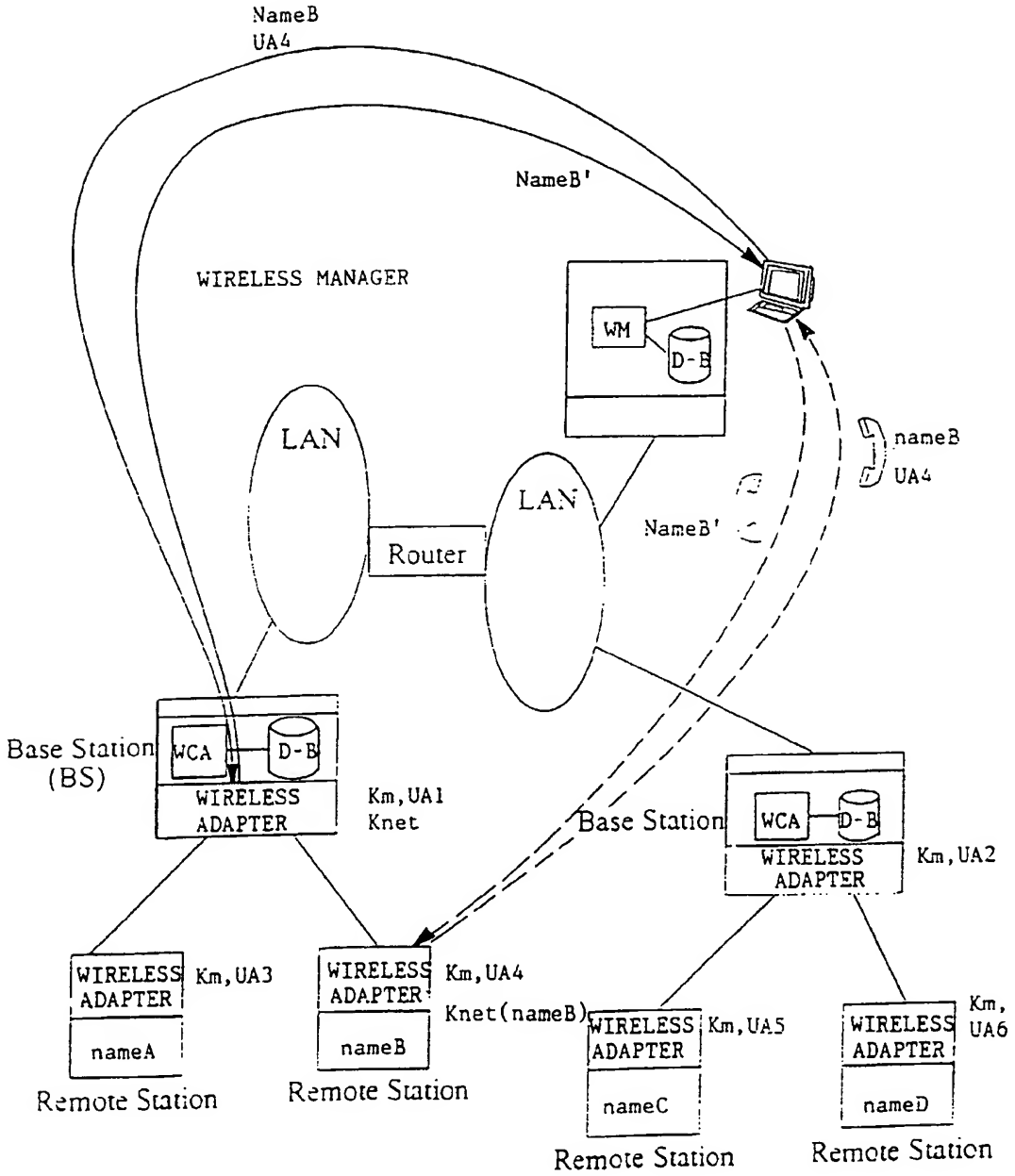
NameB
UA4
NameB'
WIRELESS MANAGER
WM
D-B
LAN
LAN
Router
nameB
UA4
NameB'
Base Station
(BS)
WCA
D-B
WIRELESS
ADAPTER
Km,UA1
Knet
Base Station
WCA
D-B
WIRELESS
ADAPTER
Km,UA2
WIRELESS
ADAPTER
Km,UA3
nameA
Remote Station
WIRELESS
ADAPTER
Km,UA4
Knet(nameB)
nameB
Remote Station
WIRELESS
ADAPTER
Km,UA5
nameC
Remote Station
WIRELESS
ADAPTER
Km,
UA6
nameD
Remote Station

FIG.2

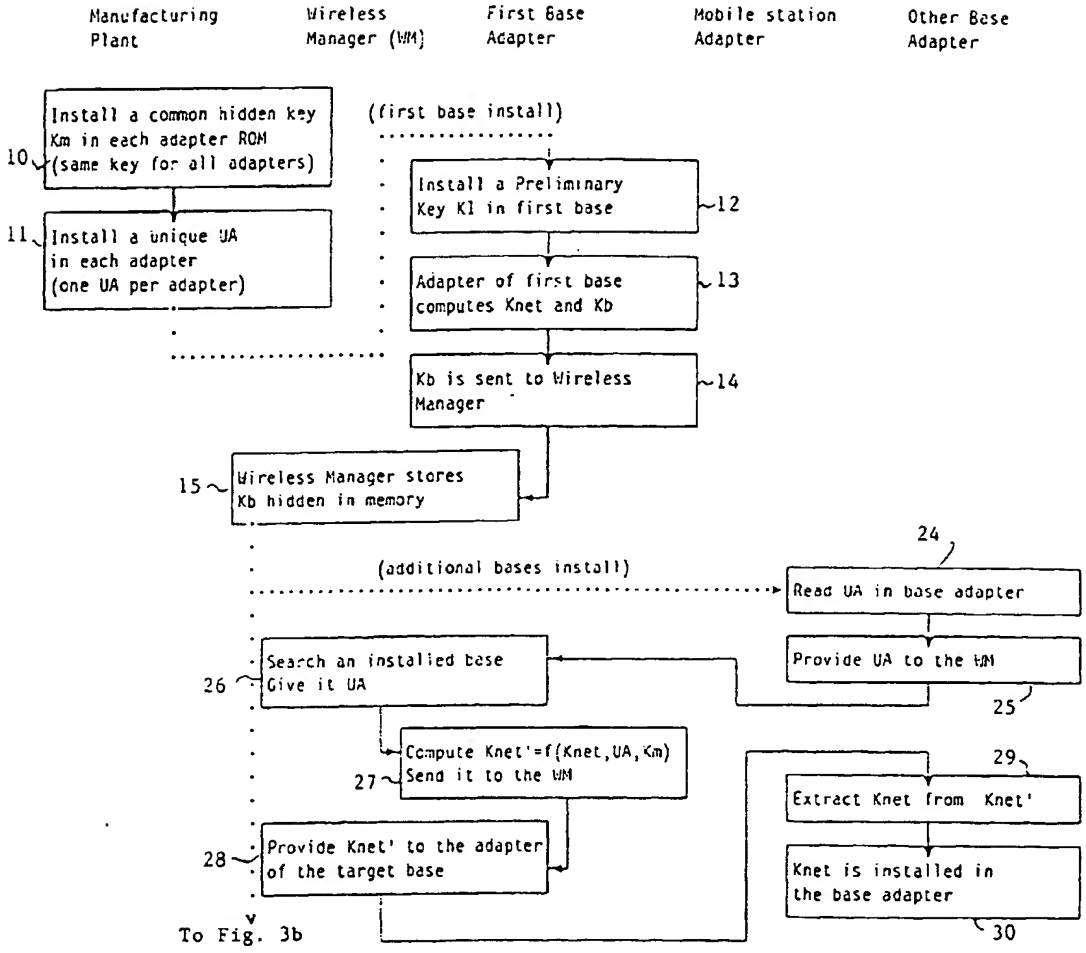
Manufacturing Plant
Wireless Manager (WM)
First Base Adapter
Mobile station Adapter
Other Base Adapter
Install a common hidden key Km in each adapter ROM (same key for all adapters)
10
Install a unique UA in each adapter (one UA per adapter)
11
(first base install)
Install a Preliminary Key KI in first base
12
Adapter of first base computes Knet and Kb
13
Kb is sent to Wireless Manager
14
Wireless Manager stores Kb hidden in memory
15
(additional bases install)
24
Read UA in base adapter
Provide UA to the WM
25
Search an installed base Give it UA
26
Compute Knet'=f(Knet,UA,Km) Send it to the WM
27
29
Extract Knet from Knet'
Provide Knet' to the adapter of the target base
28
Knet is installed in the base adapter
30
To Fig. 3b

FIGURE 3a

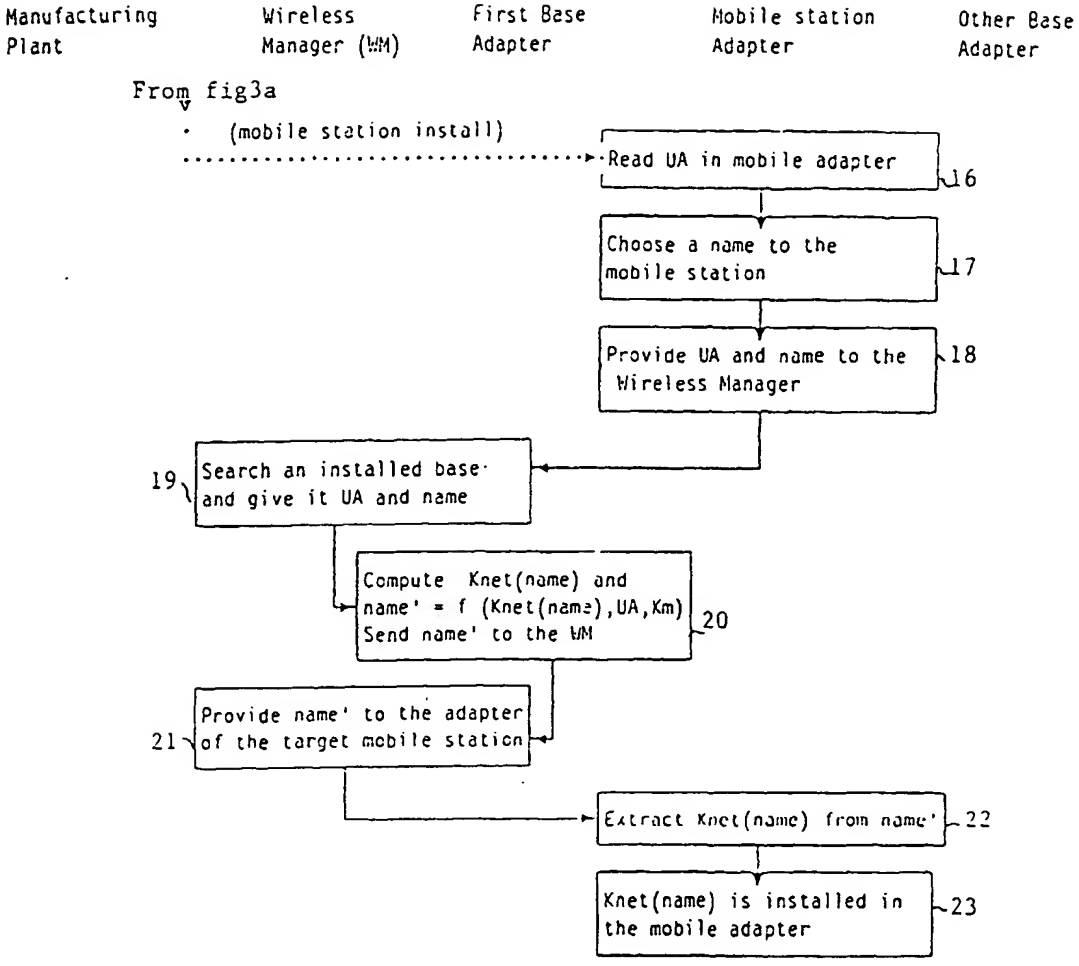
Manufacturing Plant
Wireless Manager (WM)
First Base Adapter
Mobile station Adapter
Other Base Adapter
From fig3a
(mobile station install)
Read UA in mobile adapter
16
Choose a name to the mobile station
17
Provide UA and name to the Wireless Manager
18
19
Search an installed base and give it UA and name
Compute Knet(name) and name' = f (Knet(name),UA,Km) Send name' to the WM
20
21
Provide name' to the adapter of the target mobile station
Extract Knet(name) from name'
22
Knet(name) is installed in the mobile adapter
23

FIGURE 3b

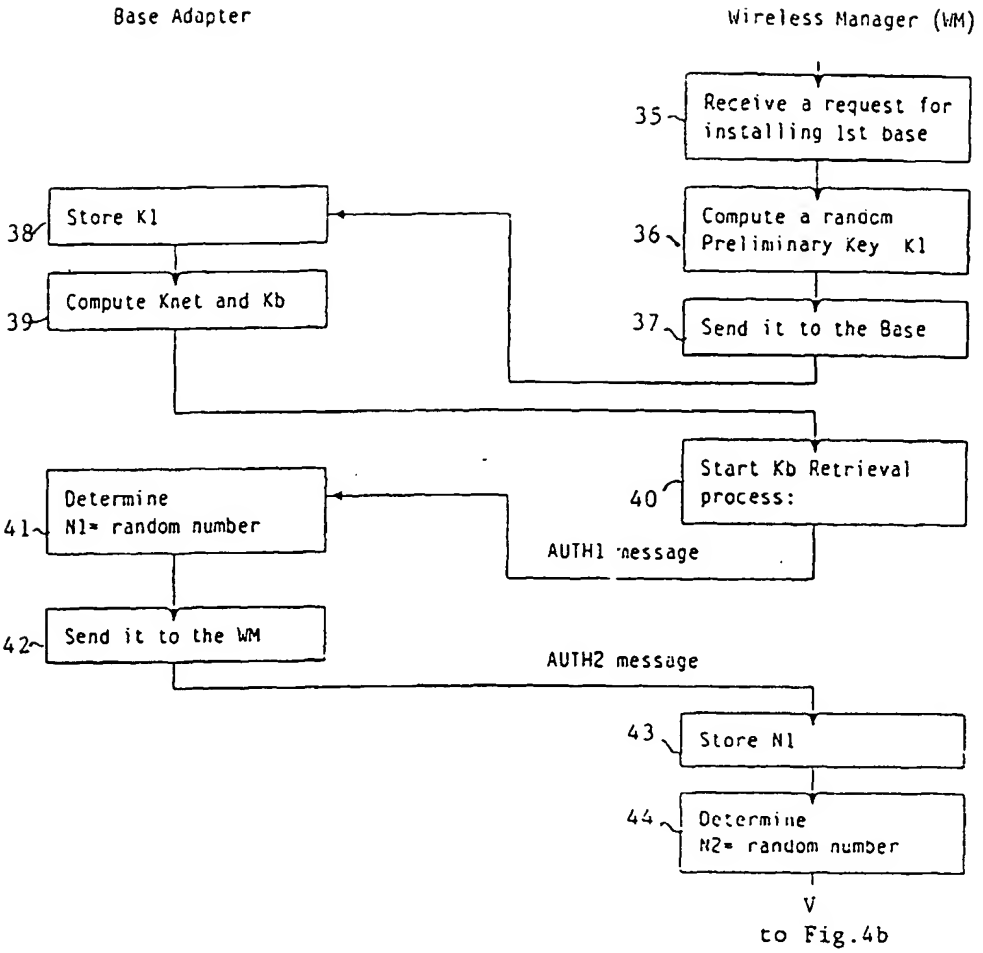
Base Adapter
Wireless Manager (WM)
35
Receive a request for installing 1st base
36
Compute a randcm Preliminary Key K1
37
Send it to the Base
38
Store K1
39
Compute Knet and Kb
40
Start Kb Retrieval process:
AUTH1 message
41
Determine N1= random number
42
Send it to the WM
AUTH2 message
43
Store N1
44
Determine N2= random number
V
to Fig.4b

FIGURE 4a

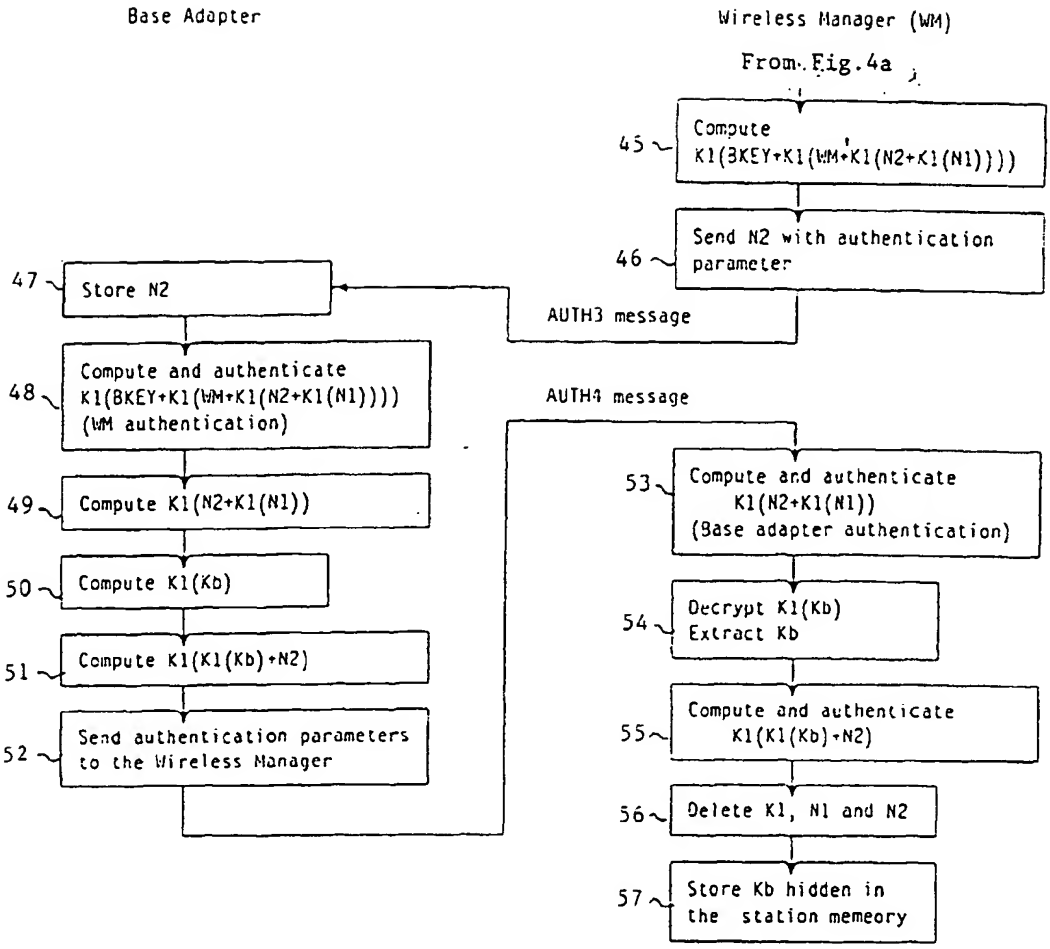
Base Adapter
Wireless Manager (WM)
From Fig.4a
45
Compute K1(BKEY+K1(WM+K1(N2+K1(N1))))
46
Send N2 with authentication parameter
AUTH3 message
47
Store N2
48
Compute and authenticate K1(BKEY+K1(WM+K1(N2+K1(N1)))) (WM authentication)
AUTH4 message
49
Compute K1(N2+K1(N1))
50
Compute K1(Kb)
51
Compute K1(K1(Kb)+N2)
52
Send authentication parameters to the Wireless Manager
53
Compute and authenticate K1(N2+K1(N1)) (Base adapter authentication)
54
Decrypt K1(Kb) Extract Kb
55
Compute and authenticate K1(K1(Kb)+N2)
56
Delete K1, N1 and N2
57
Store Kb hidden in the station memeory

FIGURE 4b

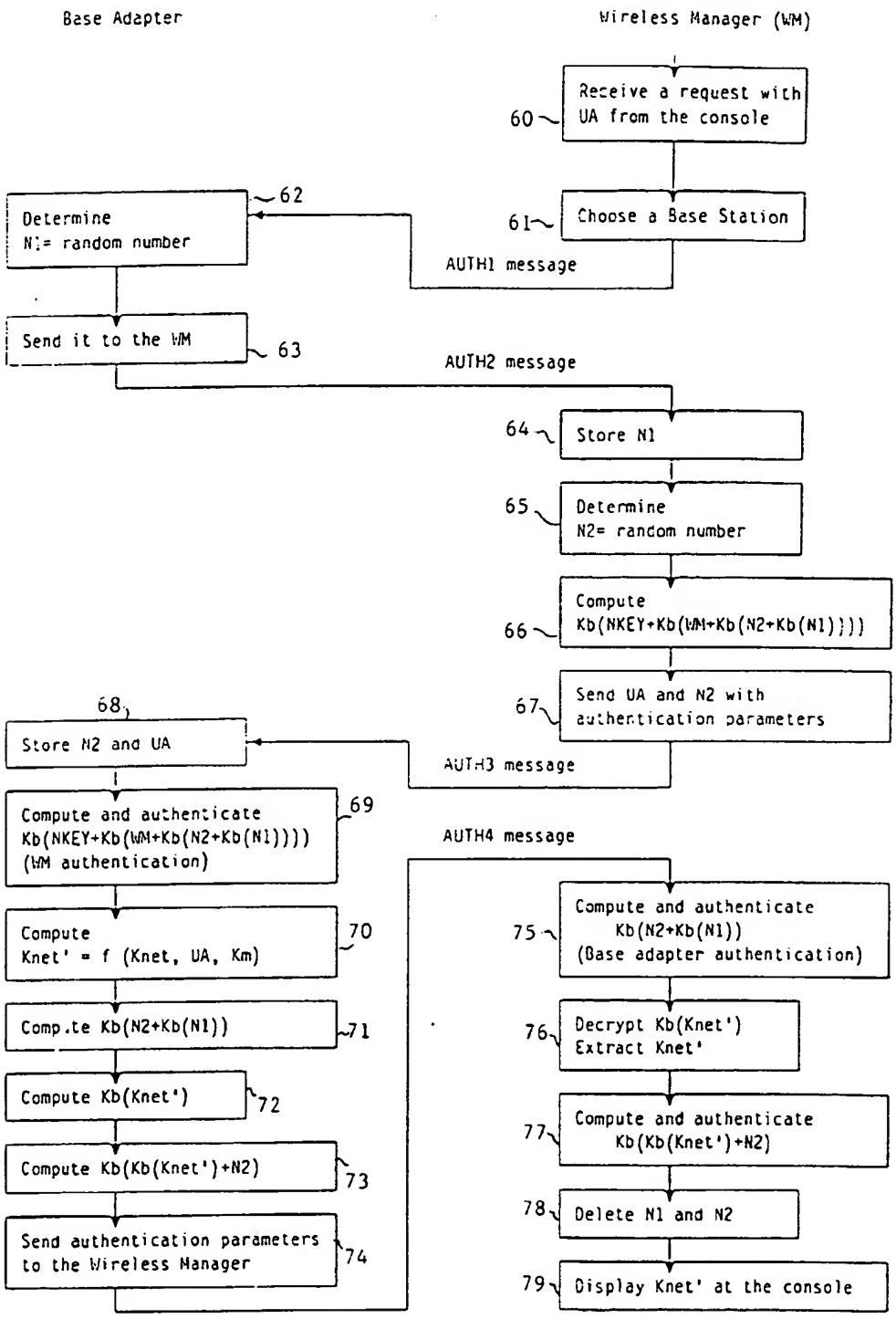
Base Adapter
Wireless Manager (WM)
Receive a request with UA from the console
60
Choose a Base Station
61
AUTH1 message
Determine N1= random number
62
Send it to the WM
63
AUTH2 message
Store N1
64
Determine N2= random number
65
Compute Kb(NKEY+Kb(WM+Kb(N2+Kb(N1))))
66
Send UA and N2 with authentication parameters
67
AUTH3 message
Store N2 and UA
68
Compute and authenticate Kb(NKEY+Kb(WM+Kb(N2+Kb(N1)))) (WM authentication)
69
AUTH4 message
Compute and authenticate Kb(N2+Kb(N1)) (Base adapter authentication)
75
Compute Knet' = f (Knet, UA, Km)
70
Decrypt Kb(Knet') Extract Knet'
76
Comp.te Kb(N2+Kb(N1))
71
Compute and authenticate Kb(Kb(Knet')+N2)
77
Compute Kb(Knet')
72
Delete N1 and N2
78
Compute Kb(Kb(Knet')+N2)
73
Display Knet' at the console
79
Send authentication parameters to the Wireless Manager
74

Figure 5

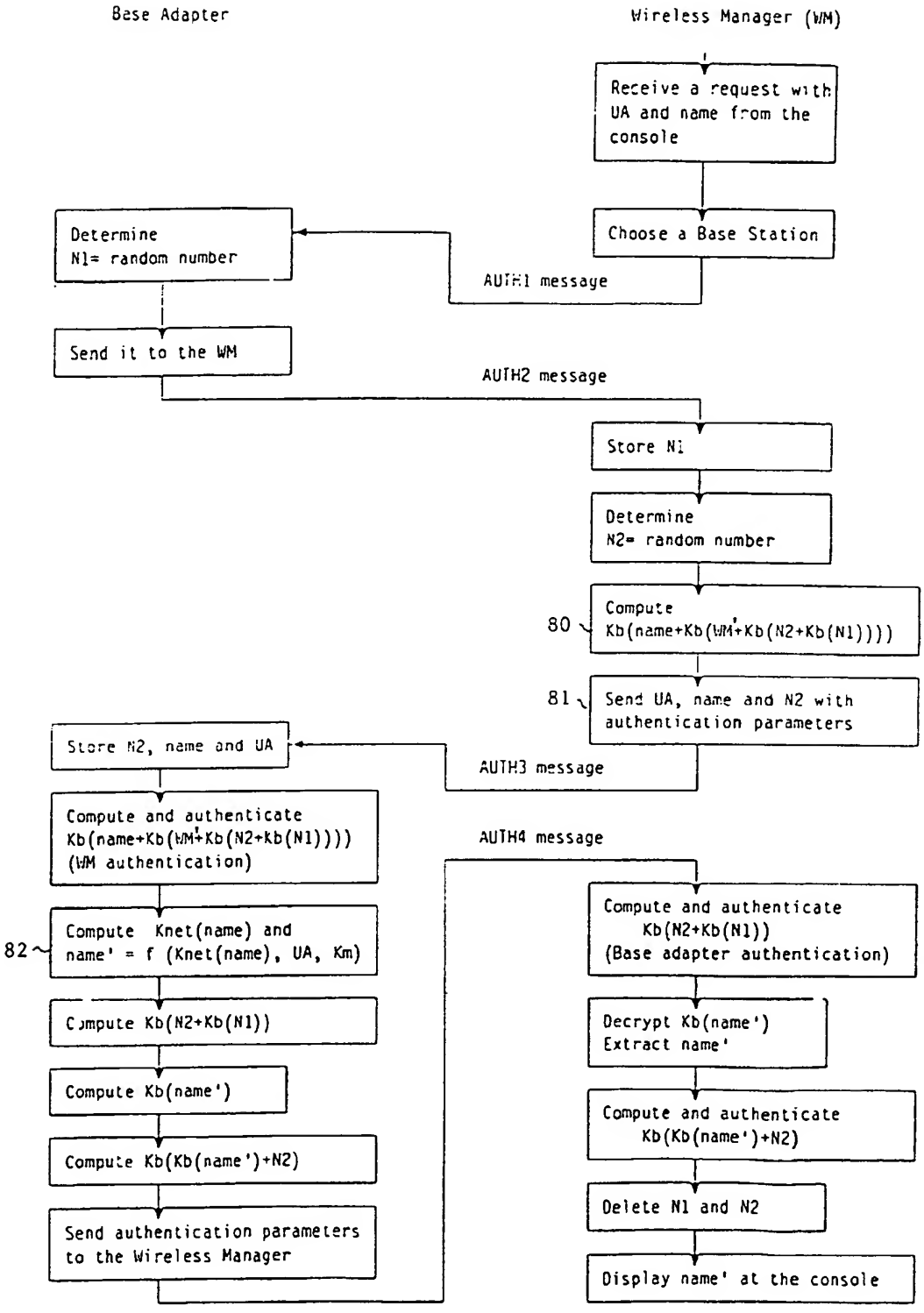
Base Adapter
Wireless Manager (WM)
Receive a request with UA and name from the console
Choose a Base Station
AUTH1 message
Determine N1= random number
Send it to the WM
AUTH2 message
Store N1
Determine N2= random number
80
Compute Kb(name+Kb(WM'+Kb(N2+Kb(N1))))
81
Send UA, name and N2 with authentication parameters
Store N2, name and UA
AUTH3 message
Compute and authenticate Kb(name+Kb(WM'+Kb(N2+kb(N1)))) (WM authentication)
AUTH4 message
82
Compute Knet(name) and name' = f (Knet(name), UA, Km)
Compute Kb(N2+Kb(N1))
Compute Kb(name')
Compute Kb(Kb(name')+N2)
Send authentication parameters to the Wireless Manager
Compute and authenticate Kb(N2+Kb(N1)) (Base adapter authentication)
Decrypt Kb(name') Extract name'
Compute and authenticate Kb(Kb(name')+N2)
Delete N1 and N2
Display name' at the console

Figure 6